Clinical Records – Audit Trails & Associated Data Corrections

Regulatory Requirements – Excerpts from Guidance Documents

INTRODUCTION

This document provides a series of excerpts from relevant regulatory guidance on audit trails and associated data corrections. The following guidance documents have been reviewed for this purpose:

1. ICH E6(R3) Guideline for Good Clinical Practice (06 January 2025)
2. ISO 14155 Clinical investigation of medical devices for human subjects — Good clinical practice (2020-07)
3. Guideline on computerised systems and electronic data in clinical trials (9 March 2023, EMA/INS/GCP/112288/2023)
4. Electronic Source Data in Clinical Investigations - FDA Guidance for Industry (September 2013)
5. Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations, Questions and Answers – FDA Guidance for Industry (October 2024, Revision 1)
6. Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims - FDA Guidance for Industry (December 2009)

ICH E6(R3) Guideline for Good Clinical Practice (06 January 2025)

2.12 Records

2.12.2 The investigator/institution should maintain adequate source records that include pertinent observations on each of the trial participants under their responsibility. Source records should be attributable, legible, contemporaneous, original, accurate and complete. Changes to source records should be traceable, should not obscure the original entry and should be explained if necessary (via an audit trail). The investigator should define what is considered to be a source record(s), the methods of data capture and their location prior to starting the trial and should update this definition when needed. Unnecessary transcription steps between the source record and the data acquisition tool should be avoided.

2.12.6 Data reported to the sponsor should be consistent with the source records or the discrepancies explained. Changes or corrections in the reported data should be traceable, should be explained (if necessary) and should not obscure the original entry.

3.11 Quality Assurance and Quality Control

3.11.4 Monitoring

3.11.4.5 Monitoring Activities

3.11.4.5.1 Communication with Parties Conducting the Trial

(c) Informing the investigator or other parties and individuals involved in the trial conduct of entry errors or omissions in source record(s) and/or data acquisition tools and ensuring that corrections, additions or deletions are made as appropriate, dated and explained (if necessary) and that approval of the change is properly documented.

3.16 Data and Records

3.16.1 Data Handling

(j) The sponsor should allow correction of errors to data, including data entered by participants, where requested by the investigators/participants. Such data corrections should be justified and supported by source records around the time of original entry.

For systems deployed by the sponsor:

(ii) Ensure that the requirements for computerised systems (e.g., requirements for validation, audit trails, user management, backup, disaster recovery and IT security) are addressed and implemented and that documented procedures and adequate training are in place to ensure the correct development, maintenance and use of computerised systems in clinical trials (see section 4). These requirements should be proportionate to the importance of the computerised system and the data or activities they are expected to process;

For systems used or deployed by the investigator/institution:

(vi) Assess whether such systems, if identified as containing source records in the trial, (e.g., electronic health records, other record keeping systems for source data collection and investigator site files) are fit for purpose or whether the risks from a known issue(s) can be appropriately mitigated. This assessment should occur during the process of selecting clinical trial sites and should be documented;

(viii) The assessment should be performed before being used in the trial and should be proportionate to the importance of the data managed in the system. Factors such as data security (including measures for backup), user management and audit trails, which help ensure the protection of confidentiality and integrity of the trial data, should be considered as appropriate;

3.16.2 Statistical Programming and Data Analysis

(e) Deviations from the planned statistical analysis or changes made to the data after the trial has been unblinded (where applicable) should be clearly documented and justified and should only occur in exceptional circumstances (e.g., data discrepancies that must be resolved for the reliability of the trial results). Such data changes should be authorised by the investigator and reflected in an audit trail. Post-unblinding data changes and deviations from the planned statistical analyses should be reported in the clinical trial report.

3.16.4 Record Access

(a) The sponsor should ensure that it is specified in the protocol or other documented agreement that the investigator(s)/institution(s) provide direct access to source records for trial-related monitoring, audits, regulatory inspection and, in accordance with applicable regulatory requirements, IRB/IEC review.

(b) The sponsor should ensure that trial participants have consented to direct access to source records for the purposes outlined in 3.16.4(a) (see section 2.8.10(n)).

4.2 Data Life Cycle Elements

4.2.2 Relevant Metadata, Including Audit Trails

The approach used by the responsible party for implementing, evaluating, accessing, managing, and reviewing relevant metadata associated with data of higher criticality should entail:

(a) Evaluating the system for the types and content of metadata available to ensure that:
  (i) Computerised systems maintain logs of user account creation, changes to user roles and permissions and user access;

(ii) Systems are designed to permit data changes in such a way that the initial data entry and any subsequent changes or deletions are documented, including, where appropriate, the reason for the change;
(iii) Systems record and maintain workflow actions in addition to direct data entry/changes into the system.

(b) Ensuring that audit trails, reports and logs are not disabled. Audit trails should not be modified except in rare circumstances (e.g., when a participant's personal information is inadvertently included in the data) and only if a log of such action and justification is maintained;
(c) Ensuring that audit trails and logs are interpretable and can support review;
(d) Ensuring that the automatic capture of date and time of data entries or transfer are unambiguous (e.g., coordinated universal time (UTC));
(e) Determining which of the identified metadata require review and retention.

4.2.3 Review of Data and Metadata

Procedures for review of trial-specific data, audit trails and other relevant metadata should be in place. It should be a planned activity, and the extent and nature should be risk-based, adapted to the individual trial and adjusted based on experience during the trial.

4.2.4 Data Corrections

There should be processes to correct data errors that could impact the reliability of the trial results. Corrections should be attributed to the person or computerised system making the correction, justified and supported by source records around the time of original entry and performed in a timely manner.

Appendix C. ESSENTIAL RECORDS FOR THE CONDUCT OF A CLINICAL TRIAL

Essential Records Table

Data and relevant metadata (including documentation of data corrections) in the data acquisition tools

Glossary

Audit Trail

Metadata records that allow the appropriate evaluation of the course of events by capturing details on actions (manual or automated) performed relating to information and data collection and, where applicable, to activities in computerised systems. The audit trail should show activities, initial entry and changes to data fields or records, by whom, when and, where applicable, why. In computerised systems, the audit trail should be secure, computer-generated and time stamped.

ISO 14155 Clinical investigation of medical devices for human subjects — Good clinical practice (2020-07)

3 Terms and definitions
3.4
audit trail
documentation that allows reconstruction of the course of events

7 Clinical investigation conduct
7.8 Document and data control
7.8.2 Recording of data
The CRFs shall be signed and dated by the principal investigator or his/her authorized designee(s). Any change or correction to data reported on a CRF shall be dated, initialled and explained if necessary, and shall not obscure the original entry (i.e. an audit trail shall be maintained); this applies to both written and electronic changes or corrections.

The sponsor shall:

a) provide guidance to the principal investigators or his/her authorized designee on making such corrections; the sponsor shall have written procedures to ensure that changes or corrections in CRFs are documented, are necessary, are legible and traceable, and are endorsed by the principal investigator or his/her authorized designee; records of the changes and corrections shall be maintained,

7.8.3 Electronic clinical data systems
Validation of electronic clinical data systems is necessary in order to evaluate the authenticity, accuracy, reliability, and consistent intended performance of the data system from design until decommissioning of the system or transition to a new system.

These requirements are applicable to any electronic records as defined in 3.21, including electronic CRFs, electronic systems used for entering and processing data from paper CRFs received from sites and other electronic systems required in the clinical investigation.

When electronic clinical databases or electronic clinical data systems are used, written procedures shall be implemented to

f) ensure that data changes are documented and that there is no deletion of entered data, i.e. maintain an audit trail, data trail and edit trail,

9 Responsibilities of the sponsor
9.2 Clinical investigation planning and conduct
9.2.4 Monitoring
9.2.4.5 Routine monitoring visits
The monitor shall perform routine monitoring activities to verify that

i) appropriate corrections, additions or deletions are made to the CRFs, dated, explained if necessary and initialled by the principal investigator or by his/her authorized designee; the monitor shall not make corrections, additions, or deletions to the CRFs,

10 Responsibilities of the principal investigator

10.6 Compliance with the CIP

The principal investigator shall

j) ensure the accuracy, completeness, legibility and timeliness of the data reported to the sponsor in the CRFs and in all required reports,

Table E.2 — Essential clinical investigation documents during clinical investigation

No.	Title of document	Purpose or comment	Site files	Sponsor files	Reference in this document
E.2.18	CRFs corrections	Gives evidence of any changes, additions, or corrections made to CRFs after data were initially recorded.	X	X	7.8.2 9.2.4.5 i) 10.6 j)

Annex J (informative) -- Clinical investigation audits

J.2 Sponsor

An audit of a sponsor's organization and documents is intended to evaluate compliance with the sponsor's own procedures, this document, and where appropriate, national regulations. The audit should include an examination of

e) clinical quality procedures (see 9.1), which address the following:

13) CRF design, data entry, and correction process;

J.3 Investigation site

An audit of the investigation site is intended to evaluate compliance with applicable agreements, sponsor procedures, EC requirements, the CIP, the requirements of this document, and where appropriate, national regulations. The audit should include an evaluation of:

i) CRFs (e.g. process of obtaining and recording information on CRFs, any corrections made to the CRFs, compliance with clinical investigation procedures);

Guideline on computerised systems and electronic data in clinical trials (9 March 2023, EMA/INS/GCP/112288/2023)

Glossary

Audit trail
In computerised systems, an audit trail is a secure, computer generated, time-stamped electronic record that allows reconstruction of the events relating to the creation, modification, or deletion of an electronic record.

4. Principles and definition of key concepts

The following sections outline the basic principles that apply to all computerised systems used in clinical trials.

4.1. Data integrity

Data integrity is achieved when data (irrespective of media) are collected, accessed, and maintained in a secure manner, to fulfil the ALCOA++ principles of being attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available when needed and traceable as described in section 4.5. in order for the data to adequately support robust results and good decision making throughout the data life cycle. Assuring data integrity requires appropriate quality and risk management systems as described in section 4.6., including adherence to sound scientific principles and good documentation practices.

- Data governance should address data ownership and responsibility throughout the data life cycle, and consider the design, operation, and monitoring of processes/systems to comply with the principles of data integrity including control over intentional and unintentional changes to data.
- Data governance systems should include staff training on the importance of data integrity principles and the creation of a working environment that enables visibility, and actively encourages reporting of omissions and erroneous results.

Lack of integrity before the expiration of the mandated retention period may render the data unusable and is equivalent to data loss/destruction.

4.3. Data and metadata

Electronic data consist of individual data points. Data become information when viewed in context. Metadata provide context for the data point. Different types of metadata exist such as: variable name, unit, field value before and after change, reason for change, trial master file (TMF) location document identifier, timestamp, user. Typically, these are data that describe the characteristics, structure, data elements and inter-relationships of data e.g. audit trails. Metadata also permit data to be attributable to an individual entering or taking an action on the data such as modifying, deleting, reviewing, etc. (or if automatically generated, to the original data source). Metadata form an integral part of the original record. Without the context provided by metadata, the data have no meaning. Loss of metadata may result in a lack of data integrity and may render the data unusable.

4.4. Source data

As a general principle, the source data should be processed as little as possible and as much as necessary.

From a practical point of view, the first obtainable permanent data from an electronic data generation/capture should be considered and defined as the electronic source data. This process should be validated to ensure that the source data generated/captured is representative of the original observation and should contain metadata, including audit trail, to ensure adherence to the ALCOA++ principles (see section 4.5.). The location where the source data is first obtained should be part of the metadata.

4.5. ALCOA++ principles

Contemporaneous

Data should be generated by a system or captured by a person at the time of the observation. The time point of the observation and the time point of the storage should be kept as part of the metadata, including the audit trail. Accurate date and time information should be automatically captured and should be linked and set by an external standard.

Complete

To reconstruct and fully understand an event, data should be a complete representation of the observation made. This includes the associated metadata and audit trail and may require preserving the original context.

Traceable

Data should be traceable throughout the data life cycle. Any changes to the data, to the context/metadata should be traceable, should not obscure the original information and should be explained, if necessary. Changes should be documented as part of the metadata (e.g. audit trail).

6. Electronic data

For each trial, it should be identified what electronic data and records will be collected, modified, imported and exported, archived and how they will be retrieved and transmitted. Electronic source data, including the audit trail should be directly accessible by investigators, monitors, auditors, and inspectors without compromising the confidentiality of participants' identities.

6.1.2. Transfer

Trial data are transferred in and between systems on a regular basis. The process for file and data transfer needs to be validated and should ensure that data and file integrity are assured for all transfers.

Data that is collected from external sources and transferred in open networks should be protected from unwarranted changes and secured/encrypted in a way that precludes disclosure of confidential information.

All transfers that are needed during the conduct of a clinical trial need to be pre-specified. Validation of transfer should include appropriate challenging test sets and ensure that the process is available and functioning at clinical trial start (e.g. to enable ongoing sponsor review of diary data, lab data or adverse events by safety committees). Data transcribed or extracted and transferred from electronic sources and their associated audit trails should be continuously accessible (according to delegated roles and corresponding access rights).

Transfer of source data and records when the original data or file are not maintained is a critical process and appropriate considerations are expected in order to prevent loss of data and metadata.

6.2. Audit trail and audit trail review

6.2.1. Audit trail

An audit trail should be enabled for the original creation and subsequent modification of all electronic data. In computerised systems, the audit trail should be secure, computer generated and timestamped.

An audit trail is essential to ensure that changes to the data are traceable. Audit trails should be robust, and it should not be possible for 'normal' users to deactivate them. If possible, for an audit trail to be deactivated by 'admin users', this should automatically create an entry into a log file (e.g. audit trail). Entries in the audit trail should be protected against change, deletion, and access modification (e.g. edit rights, visibility rights). The audit trail should be stored within the system itself. The responsible investigator, sponsor, and inspector should be able to review and comprehend the audit trail and therefore audit trails should be in a human-readable format.

Audit trails should be visible at data-point level in the live system, and it should be possible to export the entire audit trail as a dynamic data file to allow for the identification of systematic patterns or concerns in data across trial participants, sites, etc. The audit trail should show the initial entry and the changes (value - previous and current) specifying what was changed (field, data identifiers) by whom (username, role, organisation), when (date/timestamp) and, where applicable, why (reason for change).

A procedure should be in place to address the situation when a data originator (e.g. investigator or trial participant) realises that she/he has submitted incorrect data by mistake and wants to correct the recorded data.

It is important that original electronic entries are visible or accessible (e.g. in the audit trail) to ensure the changes are traceable. The audit trail should record all changes made as a result of data queries or a clarification process. The clarification process for data entered should be described and documented. Changes to data should only be performed when justified. Justification should be documented. In case the data originator is the trial participant, special considerations to data clarifications might be warranted. See Annex 5 section A5.1.1.4 for further details.

For certain types of systems (e.g. ePRO) the data entered may not be uploaded immediately but may be temporarily stored in local memory. Such data should not be edited or changed without the knowledge of the data originator prior to saving. Any changes or edits should be acknowledged by the data originator, should be documented in an audit trail and should be part of validation procedures. The timestamp of data entry in the capture tool (e.g. eCRF) and timestamp of data saved to a hard drive should be recorded as part of the metadata. The duration between initial capture in local memory and upload to a central server should be short and traceable (i.e. transaction time), especially in case of direct data entry.

Data extracts or database extracts for internal reporting and statistical analysis do not necessarily need to contain the audit trail information. However, the database audit trail should capture the generation of data extracts and exports.

Audit trails should capture any changes in data entry per field and not per page (e.g. eCRF page).

In addition to the audit trail, metadata could also include (among others) review of access logs, event logs, queries etc.

Access logs, including username and user role, are in some cases considered to be important metadata and should consequently be available. This is considered necessary e.g. for systems that contain critical unblinded data.

Care should be taken to ensure that information jeopardising the blinding does not appear in the audit trail accessible to blinded users.

6.2.2. Audit trail review

Procedures for risk-based trial specific audit trail reviews should be in place and performance of data review should be generally documented. Data review should focus on critical data. Data review should be proactive and ongoing review is expected unless justified. Manual review as well as review by the use of technologies to facilitate the review of larger datasets should be considered. Data review can be used to (among others) identify missing data, detect signs of data manipulation, identify abnormal data/outliers and data entered at unexpected or inconsistent hours and dates (individual data points, trial participants, sites), identify incorrect processing of data (e.g. non-automatic calculations), detect unauthorised accesses, detect device or system malfunction and to detect if additional training is needed

for trial participants /site staff etc. Audit trail review can also be used to detect situations where direct data capture has been defined in the protocol but where this is not taking place as described.

In addition to audit trail review, metadata review could also include (among others) review of access logs, event logs, queries, etc.

The investigator should receive an introduction on how to navigate the audit trail of their own data in order to be able to review changes.

6.3. Sign-off of data

The investigators are responsible for data entered into eCRFs and other data acquisition tools under their supervision (electronic records).

Furthermore, it is important that the investigator review the data on an ongoing basis in order to detect shortcomings and deficiencies in the trial conduct at an early stage, which is the precondition to undertake appropriate corrective and preventive actions.

Adequate oversight by the investigator is a general requirement to ensure participant safety as well as data quality and integrity. Oversight can be demonstrated by various means, one of them being the review of reported data. Lack of investigator oversight may prevent incorrect data from being corrected in a timely manner and necessary corrective and preventive actions being implemented at the investigator site.

6.6. Control of data

Data generated at the clinical trial site relating to the trial participants should be available to the investigator at all times during and after the trial to enable investigators to make decisions related to eligibility, treatment, care for the participants, etc. and to ensure that the investigator can fulfil their legal responsibility to retain an independent copy of the data for the required retention period. This

includes data from external sources, such as central laboratory data, centrally read imaging data and ePRO data.

Exceptions should be justified in the protocol e.g. if sharing this information with the investigator would jeopardise the blinding of the trial.

The sponsor should not have exclusive control of the data entered in a computerised system at any point in time. All data held by the sponsor that has been generated in a clinical trial should be verifiable to a copy of these data that is not held (or that has not been held) by the sponsor.

The requirements above are not met if data are captured in a computerised system and the data are stored on a central server under the sole control of the sponsor or under the control of a service provider that is not considered to be independent from the sponsor or if the sponsor (instead of the service provider) is distributing the data to the investigator. This is because the investigator does not hold an independent copy of the data and therefore the sponsor has exclusive control of the data. In order to meet the requirements, the investigator should be able to download a contemporaneous certified copy of the data. This is in addition to the record maintained at a service provider.

Instead of a system maintained by an independent service provider, the sponsor may take other adequate technical measures that preclude sole control. E.g. the verifiability of data (transactions) by an independent (distributed) tamper-proof ledger may provide comparable security to a system maintained by an independent service provider. This should be justified and documented.

Data entered to data acquisition tools by the investigator should be available to the investigator throughout the whole legally mandated duration and for the full duration of local legal requirements. This can be ensured either by contemporaneous local copies at the trial site or e.g. by the use of a service provider. Access to the data may be amended to read-only as part of the database lock process. Prior to read-only access to the investigator being revoked, a copy including the audit trail should be made available to the investigator in a complete and comprehensive way. In the situation where a service provider is hosting the data, the copy should not be provided via the sponsor, as this would temporarily provide the sponsor with exclusive control over the data and thereby jeopardise the investigator's control. Copies should not be provided in a way that requires advanced technical skills from the investigators. The period between the provision of the copy to the investigator and the closure of the investigators' read-only access to the database(s) should allow sufficient time for the investigator to review the copy and access should not be revoked until such a review has been performed.

Any contractual agreements regarding hosting should ensure investigator control. If the sponsor is arranging hosting on behalf of the investigators through a service provider, agreements should ensure the level of investigator control mentioned above.

Investigators delegating hosting of such data to service providers themselves should ensure that the intended use is covered by local legal requirements and the in-house rules of the institution.

6.10. Migration of data

Data, contextual information, and the audit trail should not be separated. In case migration of data into a new system results in a loss of relevant data, adequate mitigating actions should be taken to establish a robust method to join the audit trail and the data for continuous access by all stakeholders. A detailed explanation is expected, if no such method has been established to allow the migration of data and the

audit trail. Arrangements should ensure that the link between data and metadata can be established. If several parties are involved, agreements should be in place to ensure this.

6.12. Database decommissioning

After the finalisation of the trial, database(s) might be decommissioned. It is recommended that the time of decommissioning is decided taking into consideration e.g. whether the clinical trial will be used for a marketing authorisation application in the near future in which case it is recommended to keep the database(s) live. Please refer to figure 2 for a proposed approach. A dated and certified copy of the database(s) and data should be archived and available on request. In case of decommissioning, the sponsor should ensure (contractually if done by a service provider) that archived formats provide the possibility to restore the database(s). This includes the restoration of dynamic functionality and all relevant metadata (audit trail, event logs, implemented edit checks, queries, user logs, etc.). Where recommissioning is no longer possible, the sponsor should ensure that all the data including metadata files (e.g. audit trails) are available in dynamic data files. The sponsor should review the system to determine the audit trails and logs available in the system and how these would be retained as dynamic files. Where a service provider is involved, this should be addressed in the contractual arrangements. Static formats of dynamic data will not be considered adequate. See definitions section on static and dynamic formats.

A3.3 Segregation of duties

System access should be granted based on a segregation of duties and also the responsibilities of the investigator and the sponsor, as outlined in ICH E6.

Users with privileged or 'admin access' have extensive rights in the system (operating system or application), including but not limited to changing any system setting (e.g. system time), defining or deactivating users (incl. 'admin users'), activate or deactivate audit trail functionality (and sometimes even edit audit trail information) and making changes to data that are not captured in the audit trail [e.g. backend table changes in the database(s)]). There is a risk that these privileges can be misused.

Consequently, users with privileged access should be sufficiently independent from and not be involved in the management and conduct of the clinical trial and in the generation, modification, and review of data

Annex 5 Additional consideration to specific systems

A5.1 Electronic clinical outcome assessment

A5.1.1 Electronic patient reported outcome

A5.1.1.2 Data collection and data transfer

In addition to the general requirements on audit trails (please refer to section 6.2.), if an ePRO system is designed to allow data correction, the data corrections should be documented, and an audit trail should record if the data saved on the device are changed before the data are submitted.

A5.1.1.4 Data changes

As stated in section 6.2.1. on audit trails, a procedure should be in place to address and document if a data originator (e.g. investigator or trial participant) realises that they have submitted incorrect data by mistake and want to correct the recorded data.

Data changes for ePRO typically differ from that of other data acquisition tools because trial participants typically do not have the possibility to correct the data in the application. Hence, procedures need to be in place in order to implement changes when needed. This depends on the design of tools and processes and could be in the form of data clarification processes initiated by trial participants on their own reported data or initiated by investigators.

Data reported should always be reliable. Data clarification procedures introduced by the sponsor or service provider, whether or not described in the protocol should not prohibit changes in trial participant data when justified e.g. if the trial participant realises that the data have not been entered correctly.

It is expected that the possibility for changes is implemented based on a justified and trial specific risk assessment and that any changes are initiated in a timely manner by the participant or site staff and in case of the latter is based on a solid source at investigator sites e.g. phone notes or emails from trial participants documenting the communication between sites and trial participants immediately after the error was made/discovered.

One of the advantages of direct data entry by the trial participant is that recall bias is minimised as the data are entered contemporaneously. Consequently, corrections should not be done at a much later stage without good reason and justification. Whether collected on paper or by electronic means, the regulatory requirements are that all clinical data should be accurately reported and should be verifiable in relation to clinical trials.

It is expected that the number of changes to ePRO data are limited; however, this requires both designs of ePROs that are appropriate to ensure proper understanding by trial participants and appropriate training of trial participants, thereby avoiding entry errors.

A5.3 Electronic informed consent

A5.3.2 Written informed consent

There should be no ambiguity about the time of signature. The system should use timestamps for the audit trail for the action of signing and dating by the trial participant and investigator or qualified person who conducted the informed consent interview, which cannot be manipulated by system settings. Any alterations of the document should invalidate the electronic signature.

If an electronic signature is used, it should be possible for monitors, auditors, and inspectors to access the signed informed consent forms and all information regarding the signatures, including the audit trail.

Secure archiving should ensure availability and legibility for the required retention period.

A5.3.3 Trial participant identity

It should always be possible to verify the identity of a trial participant with documentation available to the investigator. Documentation which makes it possible to demonstrate that the person entering the electronic 'signature' was indeed the signatory, is required. The electronic signing should be captured by the audit trail.

Annex 6 Clinical systems

A6.1 Purchasing, developing, or updating computerised systems by sites
To ensure that system requirements related to GCP compliance (e.g. audit trail for an electronic medical record) are addressed, experienced clinical trial practitioners should be involved by the institution in the relevant steps of the procurement and validation processes.

A6.2 Site qualification by the sponsor
As part of the site qualification, the sponsor should assess the systems in use by the investigator/institution to determine whether the systems are fit for their intended use in the clinical trial (e.g. include an audit trail). The assessment should cover all computerised systems used in the clinical trial and should include consideration of the rights, safety, dignity and wellbeing of trial participants and the quality and integrity of the trial data.

A6.8 Direct access
Sponsor representatives (monitors and auditors) and inspectors should have direct, read-only access to all relevant data for all trial participants as determined by the monitors, auditors or inspectors while taking the collected data and the clinical trial protocol into account. This may require access to several different sections or modules of the respective (medical) record e.g. imaging. This requires the use of a unique identification method e.g. username and password.

The access of monitors, auditors and inspectors should be restricted to the trial participants (including potential participants screened but not enrolled in the trial) and should include access to audit trails.

Electronic Source Data in Clinical Investigations - FDA Guidance for Industry, September 2013

III. ELECTRONIC SOURCE DATA

A. Data Capture

4. Modifications and Corrections

Only a clinical investigator(s) or delegated clinical study staff should perform modifications or corrections to eCRF data. Modified and/or corrected data elements must have data element identifiers that reflect the date, time, originator and reason for the change, and must not obscure previous entries. [*see 21 CFR 11.10(e)*] A field should be provided allowing originators to describe the reason for the change (e.g., transcription error). Automatic transmissions should have traceability and controls via the audit trail to reflect the reason for the change.

B. Data Review

2. Modifications and Corrections During Clinical Investigator(s) Review of the eCRF

To comply with the requirement to maintain accurate case histories, data elements might call for modification or correction during clinical investigator(s) review. Either the clinical investigator(s) or an originator can enter the revised data element. Modified and/or corrected data elements must have data element identifiers that reflect the date, time, originator, and reason for the change, and must not obscure previous entries. [*see 21 CFR 11.10(e)*]

If changes are made to the eCRF after the clinical investigator(s) has already signed, the changes should be reviewed and electronically signed by the clinical investigator(s).

Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations, Questions and Answers – FDA Guidance for Industry (October 2024, Revision 1)

Note: *This guidance document is extensively footnoted. Please see the original document for footnotes.*

B. Electronic Systems Deployed by Regulated Entities

Q5. How should regulated entities retain electronic records from a clinical investigation?

Earlier paragraphs omitted.

As part of an inspection, FDA may request that regulated entities provide all records and data needed to reconstruct a clinical investigation, including associated metadata and audit trails.

FDA may request copies of these records (e.g., screenshots or paper printouts) and data in a human-readable form. These copies should include metadata and audit trail information. When systems are decommissioned and cannot be recommissioned or a contract with a hosted system ends, sponsors should ensure that the metadata are obtained and retained and can be linked to each corresponding data element.

Q8. What will be FDA's focus during inspections of the sponsor for electronic systems that fall under the scope of part 11, and what documentation should the sponsor have in place for such systems?

Earlier paragraphs omitted.

Consistent with a risk-based approach to validation (see Q7), sponsors should consider (1) the intended use of the system; (2) the purpose and importance of the data or records that are collected, generated, maintained, or retained in the system; and (3) the potential of the system to affect the rights, safety, and welfare of participants or the reliability of trial results to determine when documentation or SOPs addressing the following are appropriate:

- Audit trail and other information pertinent to use of the electronic system (e.g., interoperable data standards)

Q12. What are FDA's expectations for the use of audit trails by regulated entities?

Audit trails provide a means to verify the quality, authenticity, and integrity of data, allowing reconstruction of significant details about clinical investigation conduct and source data collection. Electronically generated, time-stamped audit trails, in addition to other security measures, can also capture information related to the creation, modification, or deletion of electronic records. Record changes must not obscure previously recorded information.[56]

To ensure the trustworthiness and reliability of electronic records, audit trails must capture electronic record activities including all changes made to the electronic record, the individuals making the changes, and the date and time of the changes[57] and should include the reasons for the changes. Audit trails should be protected from modification and from being disabled.

Periodic review of the audit trail may be helpful for sponsors to ensure data quality, authenticity, and integrity. The decision to review audit trails should be based on a risk assessment of the clinical investigation, considering the systems, procedures, and controls in place.

All audit trail documentation on the creation, modification, and deletion of electronic records must be available for FDA inspection.[58] A risk-based approach should be applied for retaining information on the individuals who accessed the system and the times they did so. For example, regulated entities should retain audit trail information on individual system access for electronic systems or files that contain unblinding information to verify the authenticity and integrity of the blind throughout the clinical investigation.

FDA recommends that the audit trail be retained in a format that is searchable and sortable. If this is not practical, audit trail files should be retained in a static format (e.g., PDFs) and clearly correspond to the respective data elements and/or records (see Q3 on certified copies). The information should be complete and understandable with clear and concise terms to describe the components of the audit trail. Audit trail components must include (1) the date and time the data element or information was entered or modified (see Q14), (2) the individual making the change (e.g., user ID and user role), and (3) the old value and the new value.[59] The audit trail should include the reason for the change if applicable.

The 2003 part 11 guidance states that FDA intends to exercise enforcement discretion with respect to specific part 11 requirements, including but not limited to computer-generated, timestamped audit trails.[60] Persons must still comply with all applicable predicate rules. Even where there are no predicate rule requirements related to documentation, it is nonetheless important to have audit trails or other physical, logical, or procedural security measures in place to ensure the trustworthiness and reliability of the electronic records (see Q11). FDA recommends basing a decision regarding whether to apply audit trails or other appropriate measures on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on record integrity.

Q13. Should an audit trail record every key stroke?

It is not necessary to record every key stroke in an audit trail. However, the audit trail should record deliberate actions that a user takes to create, modify, or delete electronic records (e.g., save or submit). Any edits to completed fields should be captured in the audit trail. If an edit check exists for submitted data and prompts the user to make a correction, the audit trail should include the original response, the fact that the edit check prompted a correction, and any change made in response.

Q15. What are the requirements and recommendations regarding training of individuals who use electronic systems in clinical investigations?

Anyone who develops, maintains, or uses electronic systems subject to part 11 must have the education, training, and experience necessary to perform their assigned tasks. [See § 11.10(i)] Relevant training should be provided to individuals regarding the electronic systems they will use during the clinical investigation. Training should be conducted before an individual uses the system, during the study as needed, and when changes are made to the electronic system that impact the user. Training should cover processes and procedures to access the system, to complete clinical investigation documentation, and to detect and report incorrect data. Training should be documented. Current training materials should also be available for reference to clinical trial personnel and participants during the clinical investigation. See Q8 and Q9 for more information on retention of training documentation.

C. Information Technology Service Providers and Services

Regulated entities can contract with IT service providers for IT services in a clinical investigation (e.g., data hosting, cloud computing software, platform and infrastructure services). Regulated entities are responsible for ensuring that electronic records meet applicable part 11 requirements. When determining the suitability of the IT service and IT service provider, regulated entities should consider the following regarding the IT service provider's ability to ensure the authenticity, integrity, and confidentiality of clinical investigation records and data:

- Ability to provide secure, computer-generated, time-stamped audit trails of users' actions and changes to data (see Q12)

D. Digital Health Technologies

Q20. When using DHTs to record data from participants in clinical investigations, how do sponsors identify the data originator?

As part of an audit trail, each electronic data element should be associated with an authorized data originator.[68] The data originator may be a person, a computer system, a DHT, or an "EHR" that is authorized to enter, change, or transmit data elements via a secure data transfer protocol.[69]

Q22. What should be considered during the transfer of the data from a DHT to the durable electronic data repository?

Data recorded by a DHT and any relevant associated metadata should be transmitted by a validated process to a durable electronic data repository according to the sponsor's pre-specified plan. Transmission should occur contemporaneously or as soon as possible after data are recorded. The date and time the data are transferred from the DHT to the electronic data repository should be included in the audit trail. Data stored in a durable electronic data repository can be moved to a different durable electronic data repository using a validated process.

E. Electronic Signatures

Earlier paragraphs omitted.

In addition, electronic signatures must be linked to the respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.[80] Any changes made to the record, including those subsequent to the electronic signature, must be reflected in the audit trail.[81] In situations where electronic signatures cannot be placed in a specified signature block, an electronic testament (e.g., "I approved the contents of this document") should be placed elsewhere in the document linking the signature to the electronic record.

GLOSSARY

Metadata: The contextual information required to understand the data. Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data. Examples of metadata include a date and time stamp for when the data were acquired, data originator, and other audit trail information associated with the data

Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims - FDA Guidance for Industry (December 2009)

F. Specific Concerns When Using Electronic PRO Instruments

When PRO instruments are used, sponsors must ensure that FDA regulatory requirements are met for sponsor and investigator record keeping, maintenance, and access. These responsibilities are independent of the method used to record clinical trial data and, therefore, apply to all types of PRO data including electronic PRO data. Sponsors are responsible for providing investigators with all information to conduct the investigation properly, for monitoring the investigation, for ensuring that the investigation is conducted in accordance with the investigational plan, and for permitting the FDA to access, copy, and verify records and reports relating to the investigation.

Interim paragraphs omitted

Sponsors also should avoid the following:

- Direct PRO data transmission from the PRO data collection device to the sponsor, clinical investigator, or other third party without an electronic audit trail that documents all changes to the data after it leaves the PRO data collection device.
- Clinical investigator inability to maintain and confirm electronic PRO data accuracy. The data maintained by the clinical investigator should include an audit trail to capture any changes made to the electronic PRO data at any point in time after it leaves the patient's electronic device.